REMARKS

Claims 25-28 have been amended.

The Examiner has rejected applicant's claims 25, 27 and 28 under 35 USC § 102(e) as anticipated by the Diamant, et al. patent (U. S. Patent No. 5,969,632). Claim 26 has been rejected under 35 USC § 103(a) as unpatentable based on the latter patent take with the Schneier reference (Applied Cryptography). With respect to applicant's claims, as amended, these rejections are respectfully traversed.

Applicant's independent claim 25 has been amended to better define applicant's invention. In particular, claim 25 recites a communication apparatus for transferring image data from a first network to a second network, said apparatus comprising: a first discrimination unit configured to discriminate if the received image data is confidential or not;
a judgment unit configured to judge if the transfer path to the destination of the received image data over the second network is secure or not, when the result of the discrimination by said first discrimination unit indicates the received image data is confidential; a first control unit configured to control, when the result of the discrimination by said first discrimination unit indicates the received image data is not confidential, to transfer the received image data to the destination of the received data over the second network regardless of whether the transfer path to the destination of the received image data over the second network is secure or not; and
a second control unit configured to control, when the result of the discrimination by said first discrimination unit indicates the received image data is confidential, to transfer the received image data to the destination of the received data over the second network when the result of the judgment by said judgment unit indicates the transfer path is secure, and to store the received

image data in a storage area corresponding to the destination of the received image data without transferring the received image data to the destination when the result of the judgment by said judgment unit indicates the transfer path is not secure. Claims 27 and 28 have been similarly amended.

The amended claims clearly now recite that the communication apparatus of the present invention, which transfers image data received from a first network to a second network, is arranged to control transfer of the received image data so that when the received image data is not confidential, it is transferred to the destination thereof over the second network regardless of whether the transfer path to the destination over the second network is secure or not. The communication apparatus is further arranged to control, when the received image data is confidential, transfer of the image data to the destination thereof over the second network if the transfer path is secure, and to store the image data in a storage area corresponding to the destination without being transferred to the destination if the transfer path is not secure. Accordingly, the confidentiality of the received image data is maintained as far as the received image data being confidential.

Such a construction is not taught or suggested by the cited art of record. More particularly, the Diamant, et al. patent discloses a system and method of solving the problem of unauthorized access, software viruses or the like, caused by incoming data to a computer. Specifically, in Column 10 lines 37-41 and Column 10 lines 47-59, of the Diamant, et al. patent, cited by the Examiner, one form of system and method of the patent is disclosed.

In these passages, it is stated that a transmission is stored in accordance with a mode which is judged in a step S206, if a step S204 judges that the transmission is received via a

secured network. On the other hand, if the step S204 judges that the transmission is not received via the secured network, then it is judged in a step S214 whether or not the destination of the received transmission is a secured storage area. In a case where the destination is not the secured storage area, the received transmission is stored in a public storage area in a step S216, while in a case where the destination is the secured storage area, an alert procedure is executed in a step S218.

The Examiner has also cited column 8, lines 44-51 of the Diamant, et al. patent. This passage states, in part, as follows: "Thus, information can be stored in the secured storage area 18 in two cases, either if at least partially received from the secure network 8 or if originally determined as confidential information by one of the computers 20, 30 and 40, connected to the secured network 8."

Thus, in the system of the Diamant, et al. patent, if the transmission is over the secured network, the storage is according to one of the methods for storing data in the secured storage area 18 and/or the public storage area 16. Column 8, line 44 through Column 9, line 6. If the transmission is not received over the secured network and the destination is not the secured storage area, the data is stored in the public storage area, but if the destination is the secured storage area, an alert procedure is executed.

The above system and method of the Diamant, et al. patent, therefore, deal with the storage of the received data in public and/or secured storage areas. This is very different from applicant's claimed invention which deals with whether or not and how data is to be transferred over a second network from a first network.

More importantly, in the above system and method of the Diamant, et al. patent, the

storage of data depends upon whether transmission is over the secured network or not and, if not, also upon the destination. In contrast, in applicant's claimed invention, transmission over the second network depends upon whether the information is confidential or not and, if confidential, also depends upon whether the second network is secure or not.

More particularly, in the above system and method of the Diamant, et al patent, if the transmission is not over the secured network, then whether or not the destination of the received transmission is the secured storage area is determined. This is quite different from applicant's claimed invention in which, if the received image data is not confidential, the received image data is transferred via the second network regardless of whether the transfer path over the second network is secure.

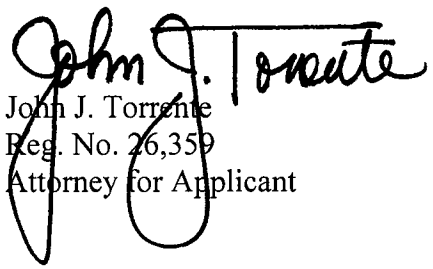
Additionally, in the above system and method of the Diamant, et al patent, if the transmission is received over the secured network, the transmission is stored either in the secured storage area or in the secured storage area and the public storage area in accordance with the mode. This again is considerably different from applicant's claimed invention in which, if the received image data is confidential, it is judged whether the transfer path over the second network is secure, so that if the transfer path is secure, the received image data is transferred via the second network, and if not secure, the received image data is stored in the storage area corresponding to the destination without being transferred to the destination.

Applicant's amended independent claims 25, 27 and 28, and their respective dependent claims, all of which recite the above features thus patentably distinguish over the Diamant, et al. patent. The Schneier reference adds nothing to the Diamant, et al. patent to change this conclusion.

In view of the above, it is submitted that applicant's claims, as amended, patentably distinguish over the cited art of record. Accordingly reconsideration of the claims is respectfully requested.

Dated: December 6, 2007

Respectfully submitted,



COWAN, LIEBOWITZ & LATMAN
1133 Avenue of the Americas
New York, New York 10036
T (212) 790-9200

John J. Torrente
Reg. No. 26,359
Attorney for Applicant